

534 Rec'd PCT/PTC 14 JUL 2000

METHOD FOR OPERATING A VEHICLE, AND A DEVICE FOR CARRYING
OUT SAID METHOD

The invention relates to a method for operating a vehicle and to a device for carrying out the method.

The method according to the invention is based on a method having the characteristics of the preamble of Claim 1.

A method of this type is known from German Patent Document DE 36 15 890 A. In that document, the dialogue between the control device and the authorization verification device (BNE) is carried out in a wireless manner. The authorization verification device is, for example, a transponder which receives an interrogation signal emitted by the control device and emits a response signal with a response code. If the user is authorized, the control device recognizes this user because of the correct response code and permits or implements the unlocking of the vehicles doors. In the case of the known method, it will then be easily possible to start the vehicle drive unit. A rotary button provided for this purpose is combined with the steering wheel lock and can easily be operated. The problem arises in this case that, for starting the vehicle drive unit, it is sufficient to unlock the

vehicle. A vehicle passenger can therefore also start the operation of the vehicle drive unit if the authorized vehicle user carrying the BNE does not want him to do so.

The described problem becomes particularly serious when the access authorization is queried in a form known from German Patent Document DE 195 16 316 A. There the question-answer dialogue is already carried out when the authorized user approaches the door handle with his hand. If he does this, for example, not with the intention of opening the vehicle door and does not recognize that the dialogue has nevertheless resulted in his identification and the vehicle is unlocked, it will then be possible for a third party to enter the vehicle and start the drive unit without the authorized user's knowledge.

In addition to the known method, it will in the future also be possible to verify the access authorization by individual body-related characteristics. An identification is known, for example, which takes place by means of a finger print or a speech recognition. Also in the case of such a physiological authorization verification device, in the quasi automatic clearing of the vehicle drive unit known from German Patent Document DE 36 15 890 A, there is the problem of an undesired or unauthorized start of the operation of the this unit.

It is an object of the invention to provide a method of the initially mentioned type in which this problem is eliminated.

The invention achieves this object by means of the characteristics of Claim 1.

Because the authorization to start the operation of the vehicle drive unit is now no longer coupled to a mechanical ignition key, the problem of a loss of the memory during the operation of the vehicle drive unit occurs particularly when an electronic memory is provided for the access authorization verification. This loss may be unnoticed by the authorized user; for example, in that the memory is removed unnoticed from the vehicle.

The same problem occurs when the memory loses its capacity to transmit the access authorization code. For example, in the event of an electric defect of the BNE, which occurs during the operation of the vehicle drive unit, the BNE will be ineffective and will no longer permits the subsequent start of the operation of the vehicle drive unit. This takes place, for example, if the drive unit is constructed as an internal-combustion engine and the latter must be stopped for a short time in front of a closed grade crossing.

Because the access code must be transmitted for the start of the operation of the vehicle drive unit, this results in a considerable problem for the vehicle user. In order to avoid this problem, the query of the access code can also take place during and/or after the conclusion of the operation of the vehicle drive unit. The query during the operation makes it possible to rapidly detect the loss. The prerequisite is only a corresponding frequency of the query.

The query after the conclusion of the operation permits at least the taking of appropriate measures in order to then be able to start the vehicle again. The result of the query of the access code during or after the conclusion of the operation of the vehicle drive unit may be the emission of a warning signal. With respect to the above, it is advantageous to provide in this case a vehicle-fixed memory for the access code which will then be unlocked and can, for example, also be removed from the vehicle by the user.

This memory is provided in addition to the actual memory for the access code. This redundant memory will then be operative. It may be constructed as a mechanical part which is inserted in the authorization verification device and functionally replaces the memory for the access code provided there which may be defective. The memory can then be inserted alone or together with the BNE in an activating part for the

start of the operation or the operation of the vehicle drive unit. It can also be connected with a mechanical key which is then placed in an ignition lock and permits the start of the operation of the vehicle drive unit in the conventional manner.

In order to indicate to the vehicle user that the redundant memory has become effective, the vehicle user can be conspicuously informed of the implemented unlocking of the vehicle-fixed memory. This clearly reduces the danger of an accidental leaving of the redundant memory in the vehicle and the related possibility of a start of the vehicle by the unauthorized user.

If, in the process, the memory is ejected out of its receiving device, this special situation is not only clearly pointed out to the vehicle user but is also caused to pay special attention to the locking operation of the vehicle and to optionally carry out the locking conventionally, for example, by means of a mechanical key which, as a rule, is also present.

This eliminates the risk of enabling in an emergency by the measures provided for this purpose an unauthorized person to use the vehicle. The authorized user is caused to carry out the required measures (such as the removal of the

SECRET

Figure 1 is a frontal view of an activating unit for a vehicle drive unit;

Figure 3 is a top view of the authorization verification device of Figure 2 supplemented by a constructional unit which permits the start of the operation of the vehicle drive unit in the event of an emergency.

6

which is also not shown, is started. As a result, the drive unit, here assumed to be an internal-combustion engine, can be started.

It is important in this case that the starting in the normal situation, that is, when the existing components are operating properly, the starting takes place without inserting a conventional ignition key in the activating unit 1.

In order to check the authorization for starting the operation of the drive unit, an authorization verification device 5 is provided which contains a memory (not shown) for an access authorization code and which, in addition, is constructed in the conventional manner as a remote control signal generator. It has push buttons 6 and 7 for the remote unlocking of the central locking system (6) or of the trunk (7) as well as additionally a push button 8 for emitting a remote control signal for locking the doors and the flaps of the vehicle. When the push button 6 or 7 is activated, the memory for the access authorization code is read out and emits in a known manner the authorization verification code which also changes in a known manner with each activation corresponding to a defined algorithm and therefore ensures a protection against monitoring. The code is received by a control unit provided in the vehicle. If it corresponds to the expected code, the corresponding remote control command is

implemented.

It is also provided that a previously closed vehicle can be opened without the emission of a remote control signal. As known per se from German Patent Document DE 35 36 377 A, for this purpose, a dialogue is triggered between the control unit and the device 5 when a door handle is operated and, if the expected code is emitted by the device 5, the locking of the vehicle is eliminated and the access is permitted.

For starting the operation of the drive unit, by means of the rotating of part 2 in the direction of the arrows 3 and 4, an interrogation signal is also emitted which is received by the device 5 and, as described above, in the case of the question-and-answer dialogue for the access, is answered by the emission of the access authorization code. The control unit receives this code and, if it corresponds to the expected code, enables the ignition current and starter current circuit.

As a result, it is possible to start the vehicle without using a conventional mechanical ignition key. On the other hand, by the query of the access authorization code before the start of the operation of the drive unit, it is ensured that the unit 5 is situated inside the vehicle. Thus ensures that the user who has accessed the vehicle in an authorized manner,

is now most probably sitting inside the vehicle; that is, the start of the operation of the vehicle drive unit most probably is initiated by him or at least with his approval.

For the event that, after the drive unit has been started, the unit 5 is removed from the vehicle or becomes inoperative, an additional measure is provided. This measure first consists of querying the authorization code at defined points in time. This may take place when the drive unit is switched off. However, it may also occur when the drive unit is restarted without a previous opening and closing of a vehicle door, or also at regular time intervals during the operation of the drive unit. For this purpose, the access authorization code is always queried by the control unit and, if the unit 5 is disposed inside the vehicle and is operative, the verification of the authorization and of the operatability of the unit 5 is supplied by the emission of the access authorization code.

In the assumed fault cases, the access authorization code will no longer be emitted upon the query. In order to even then still ensure the proper operation of the vehicle and permit the restarting of the drive unit, an additional memory 9 is provided inside the device 1, which memory 9 also contains the access authorization code and which is locked inside the device 1. In the event of the described emergency,

the locking (not shown) is eliminated. The memory 9 can therefore be removed from the device 1.

The memory 9 forms a constructional unit with a mechanical key 10 which can be fitted into the unit 5. This is illustrated in Figure 3. In this case, the memory 9 replaces the memory provided in the unit 5. This memory 9 supplies the access authorization code which is emitted by the unit 5, either by the operation of the push buttons 6 or 7 or upon the interrogation signal of the control unit.

If the energy accumulator (not shown) provided in the unit 5 is spent, a remote control signal cannot be emitted. Thus, a vehicle door can only be unlocked mechanically. This takes place in that the key 10 is pushed into a corresponding receiving device of a vehicle door lock.

Likewise, it is possible to start the drive unit in this case. For this purpose, the unit consisting of parts 9 and 10 is fitted into the device 5. Like a conventional ignition key, the key 10 is then used for permitting the starting of the operation of the drive unit by rotating the rotatable part 2. The opening and the starting of the vehicle can therefore take place conventionally at any time.